Complementation in the Group of Units of Matrix Rings

Stewart Wilcox

ABSTRACT

Let R be a ring with 1 and $\mathcal{J}(R)$ its Jacobson radical. Then $1 + \mathcal{J}(R)$ is a normal subgroup of the group of units, $G(R)$. The existence of a complement to this subgroup was explored in a paper by Coleman and Easdown; in particular the ring $R = \mathrm{Mat}_n(\mathbb{Z}_{p^k})$ was considered. We prove the remaining cases to determine for which n, p and k a complement exists in this ring.

1. INTRODUCTION

If R is a ring with 1, let $G(R)$ denote its group of units. If $\psi : R \to S$ is a ring homomorphism which maps $1_R \mapsto 1_S$, let $G(\psi) : G(R) \to G(S)$ denote the corresponding group homomorphism. Denoting by $\mathcal{J}(R)$ the Jacobson radical of R, it can be shown that $J(R) = 1+\mathcal{J}(R)$ is a normal subgroup of $G(R)$. In [2] results were found about the existence of a complement of $J(R)$. In particular these were applied to partly classify the case when $R = \mathrm{Mat}_n(\mathbb{Z}_{p^k})$ for a prime p and integers $n, k \geq 1$. The remaining values of p, n and k are considered in Propositions 4 and 5 to give the following results.

Theorem 1. *Let $R = \mathrm{Mat}_n(\mathbb{Z}_{p^k})$. Then $J(R)$ has a complement in $G(R)$ exactly when*

- *$k = 1$, or*
- *$k > 1$ and $p = 2$ with $n \leq 3$, or*
- *$k > 1$ and $p = 3$ with $n \leq 2$, or*
- *$k > 1$ and $p > 3$ with $n = 1$.*

When $k = 1$ the subgroup $J(R)$ is trivial, and so complemented. Theorems 4.3 and 4.5 of [2] can be summarised as

Theorem 2 (Coleman-Easdown)**.** *Define R as above. If $p = 2$ or 3 and $n = 2$, then $J(R)$ has a complement in $G(R)$. If $p > 3$, $n \geq 2$ and $k \geq 2$ then $J(R)$ has no complement.*

It is well known (see, for example, Theorem 11.05 of [3]) that there exists $a \in \mathbb{Z}_{p^k}$ with order $p-1$. The subgroup generated by a then complements

2000 *Mathematics Subject Classification.* Primary 16U60

$1 + p\mathbb{Z}_{p^k}$ in $G(\mathbb{Z}_{p^k})$, so a complement always exists when $n = 1$. Thus it remains to prove existence when $p = 2$ with $n = 3$, and disprove existence when $p = 2$ with $n \geq 4$ and $p = 3$ with $n \geq 3$. Before proving Propositions 4 and 5, we make some preliminary observations. Since $\mathbb{Z}_{p^k}$ is local, clearly $\mathcal{J}(\mathbb{Z}_{p^k}) = p\mathbb{Z}_{p^k}$ and $\mathbb{Z}_{p^k}/\mathcal{J}(\mathbb{Z}_{p^k}) \cong \mathbb{Z}_p$. Let $\phi_k : \mathbb{Z}_{p^k} \twoheadrightarrow \mathbb{Z}_p$ be the natural surjection. From Theorem 30.1 of [4], we have

$$\mathcal{J}(\mathrm{Mat}_n(S)) = \mathrm{Mat}_n(\mathcal{J}(S))$$

for any ring S. In particular with $R = \mathrm{Mat}_n(\mathbb{Z}_{p^k})$ as above,

$$\mathcal{J}(R) = \mathrm{Mat}_n(\mathcal{J}(\mathbb{Z}_{p^k})) = \mathrm{Mat}_n(p\mathbb{Z}_{p^k})$$

so that

$$R/\mathcal{J}(R) \cong \mathrm{Mat}_n(\mathbb{Z}_p)$$

Let $\psi_{n,k} : R \twoheadrightarrow \mathrm{Mat}_n(\mathbb{Z}_p)$ be the corresponding surjection, which is induced by ϕ_k in the obvious way. Then $G(\psi_{n,k})$ is surjective with kernel $J(R)$. Thus $J(R)$ is complemented in $G(R)$ if and only if there exists a group homomorphism $\theta : \mathrm{GL}_n(\mathbb{Z}_p) \to G(R)$ with $G(\psi_{n,k})\theta = \mathrm{id}_{\mathrm{GL}_n(\mathbb{Z}_p)}$.

2. NONEXISTENCE

We first reduce to the case $k = 2$ and n minimal.

Lemma 3. *Assume $k > 1$ and let $R = \mathrm{Mat}_n(\mathbb{Z}_{p^k})$ as above. Pick any $m \leq n$. If $J(R)$ has a complement in $G(R)$, then $J(S)$ has a complement in $G(S)$ where $S = \mathrm{Mat}_m(\mathbb{Z}_{p^2})$.*

Proof. Since $J(R)$ has a complement, the discussion of the previous section shows that there exists $\theta' : \mathrm{GL}_n(\mathbb{Z}_p) \to G(R)$ with

$$G(\psi_{n,k})\theta' = \mathrm{id}_{\mathrm{GL}_n(\mathbb{Z}_p)}$$

We have a ring homomorphism $\lambda : \mathbb{Z}_{p^k} \twoheadrightarrow \mathbb{Z}_{p^2}$ satisfying $\phi_2\lambda = \phi_k$. Then λ induces $\mu : \mathrm{Mat}_n(\mathbb{Z}_{p^k}) \twoheadrightarrow \mathrm{Mat}_n(\mathbb{Z}_{p^2})$, which satisfies $\psi_{n,2}\mu = \psi_{n,k}$. Thus

$$\mathrm{id}_{\mathrm{GL}_n(\mathbb{Z}_p)} = G(\psi_{n,k})\theta' = G(\psi_{n,2})G(\mu)\theta' = G(\psi_{n,2})\theta$$

where $\theta = G(\mu)\theta'$. Denote $\psi_{n,2}$ by ψ_n. Let $H \leq \mathrm{GL}_n(\mathbb{Z}_p)$ be the subgroup consisting of all matrices of the form

$$\begin{pmatrix} A & 0 \\ 0 & I_{n-m} \end{pmatrix}$$

where $A \in \mathrm{GL}_m(\mathbb{Z}_p)$ and I_{n-m} is the identity matrix of size $n-m$. Then $H' = \psi_n^{-1}(H)$ contains $\theta(H)$, and consists of those invertible matrices $A = (a_{ij})$ which satisfy $a_{ij} - \delta_{ij} \in p\mathbb{Z}_{p^2}$ whenever $i > m$ or $j > m$. Pick elements $A = (a_{ij})$ and $B = (b_{ij})$ of H', and assume $i, j \leq m$ but $l > m$. Clearly $\delta_{il} = \delta_{lj} = 0$ so that $a_{il}, b_{lj} \in p\mathbb{Z}_{p^2}$. Hence $a_{il}b_{lj} = 0$, so that for $i, j \leq m$ we have

$$(ab)_{ij} = \sum_{l=1}^{n} a_{il}b_{lj} = \sum_{l=1}^{m} a_{il}b_{lj}$$

Thus mapping the matrix $A = (a_{ij})_{1\leq i,j\leq n} \in H'$ to $(a_{ij})_{1\leq i,j\leq m}$ gives a homomorphism $\nu : H' \to G(\mathrm{Mat}_m(\mathbb{Z}_{p^2}))$. But there is an obvious isomorphism $\kappa : \mathrm{GL}_m(\mathbb{Z}_p) \to H$ and this satisfies

$$\psi_m \nu \theta \kappa = \mathrm{id}_{\mathrm{GL}_m(\mathbb{Z}_p)}$$

noting that the image of $\theta\kappa$ lies in the domain of ν. Since $\theta_1 = \nu\theta\kappa$ is a homomorphism, the result follows. $\square$

Proposition 4. *Assume $k > 1$ and define R as above. If $p = 2$ with $n \geq 4$, or $p = 3$ with $n \geq 3$, then $J(R)$ has no complement in $G(R)$.*

Proof. By the previous Lemma, we may assume that $k = 2$, and that $n = 4$ when $p = 2$ and $n = 3$ when $p = 3$. First take the $p = 3$ case, and consider the following two elements of $\mathrm{GL}_3(\mathbb{Z}_3)$

$$\alpha = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad \text{and} \qquad \beta = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

It is easy to verify that $\alpha^3 = 1$ and $\alpha\beta = \beta\alpha$. Since $\psi_3\theta = \mathrm{id}$ we may write

$$\begin{aligned} \theta(\alpha) &= \begin{pmatrix} 3a+1 & 3b+2 & 3c \\ 3d & 3e+1 & 3f \\ 3g & 3h & 3i+1 \end{pmatrix} \\ \theta(\beta) &= \begin{pmatrix} 3p+1 & 3q & 3r+2 \\ 3s & 3t+1 & 3u \\ 3v & 3w & 3x+1 \end{pmatrix} \end{aligned}$$

where all variables are integers. Then entry $(1, 2)$ of $\theta(\alpha^3) = \theta(1)$ gives $d = 1 \pmod 3$, while entry $(2, 3)$ of $\theta(\alpha\beta) = \theta(\beta\alpha)$ gives $d = 0 \pmod 3$,

clearly a contradiction. Now assume $p = 2$, and consider the following two elements of $\mathrm{GL}_4(\mathbb{Z}_2)$

$$\alpha = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad \text{and} \qquad \beta = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

It is easy to verify that $\alpha^2 = \beta^2 = 1$ and $\alpha\beta = \beta\alpha$. Since $\psi_4\theta = \mathrm{id}$ we may write

$$\theta(\alpha) = \begin{pmatrix} 2a+1 & 2b & 2c+1 & 2d \\ 2e & 2f+1 & 2g+1 & 2h+1 \\ 2i & 2j & 2k+1 & 2l \\ 2m & 2n & 2o & 2p+1 \end{pmatrix}$$

and

$$\theta(\beta) = \begin{pmatrix} 2q+1 & 2r & 2s & 2t+1 \\ 2u & 2v+1 & 2w+1 & 2x \\ 2y & 2z & 2A+1 & 2B \\ 2C & 2D & 2E & 2F+1 \end{pmatrix}$$

where again all variables are integers. After a lengthy calculation, from entries $(1,3)$, $(1,4)$ and $(2,4)$ of $\theta(\alpha^2) = 1$ we obtain

$$\begin{aligned} a+b+k &= 1 \pmod 2 \\ b+l &= 0 \pmod 2 \\ f+l+p &= 1 \pmod 2 \end{aligned}$$

Similarly from entries $(1,3)$, $(2,3)$ and $(2,4)$ of $\theta(\beta^2) = 1$ we obtain

$$\begin{aligned} E+r &= 0 \pmod 2 \\ A+v &= 1 \pmod 2 \\ B+u &= 0 \pmod 2 \end{aligned}$$

Finally comparing entries $(1,4)$ and $(2,3)$ of $\theta(\alpha\beta) = \theta(\beta\alpha)$,

$$a+B+p+r = 0 \pmod 2 \qquad \text{and} \qquad A+E+f+k+u+v = 0 \pmod 2$$

Summing the above 8 equations gives $0 = 1 \pmod 2$, and we have the required contradiction. $\square$

3. EXISTENCE

Proposition 5. *Assume $k > 1$ and define R as above. If $p = 2$ and $n = 3$ then $J(R)$ has a complement in $G(R)$.*

Proof. The group $GL_3(\mathbb{Z}_2)$ has the following presentation, which can be easily verified using a standard computer algebra package such as MAGMA [1],

$$GL_3(\mathbb{Z}_2) = \langle \alpha, \beta \mid \alpha^2 = \beta^3 = (\alpha\beta)^7 = (\alpha\beta\alpha\beta^{-1})^4 = 1 \rangle$$

where

$$\alpha = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad \text{and} \qquad \beta = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

We will construct a homomorphism $\theta : \mathrm{GL}_3(\mathbb{Z}_2) \to \mathrm{GL}_3(\mathbb{Z}_{2^k})$ such that

$$G(\psi_{3,k})\theta = \mathrm{id}_{\mathrm{GL}_3(\mathbb{Z}_2)} \tag{1}$$

Now there exists a with $a = 1 \pmod 2$ and $a^2 + a + 2 = 0 \pmod{2^k}$ by Hensel's Lemma. Define $\bar{\alpha}, \bar{\beta} \in \mathrm{GL}_3(\mathbb{Z}_{2^k})$ by

$$\bar{\alpha} = \begin{pmatrix} 1 & a & -a-1 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \quad \text{and} \quad \bar{\beta} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

It is easily verified using $a^2 + a + 2 = 0 \pmod{2^k}$ that

$$\bar{\alpha}^2 = 1 \quad \bar{\beta}^3 = 1 \quad (\bar{\alpha}\bar{\beta})^7 = 1 \quad (\bar{\alpha}\bar{\beta}\bar{\alpha}\bar{\beta}^{-1})^4 = 1$$

We can then define θ by $\theta(\alpha) = \bar{\alpha}$ and $\theta(\beta) = \bar{\beta}$. Then (1) holds for α and β, since $a = 1 \pmod 2$. But α and β generate $\mathrm{GL}_3(\mathbb{Z}_2)$, so (1) holds. The result then follows by the observations of Section 1. □

ACKNOWLEDGEMENTS

This work was completed while the author was a recipient of a vacation scholarship from the School of Mathematics and Statistics, University of Sydney.

References

[1] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. http://magma.maths.usyd.edu.au/magma/.

[2] Clare Coleman and David Easdown. Complementation in the group of units of a ring. *Bull. Austral. Math. Soc.*, 62(2):183–192, 2000.

[3] Ian D. Macdonald. *The theory of groups*. Robert E. Krieger Publishing Co. Inc., Malabar, FL, 1988. Reprint of the 1968 original.

[4] F. A. Szász. *Radicals of rings*. John Wiley & Sons Ltd., Chichester, 1981. Translated from the German by the author, A Wiley-Interscience Publication.